The annotation **[2E]** denotes two Engagement Marks, of which there are supposed to be 24 for a student who attempts all of Section A and two questions from Section B. **B**, **S** and **U** means bookwork, seen and unseen, but the boundaries between those are not very sharp.

Section A

1. In this question, G is a group and X is a set.

(a) Define what is meant by an *action* of G on X. [2]

A. *An action of G on X is a map $a\colon G \times X \to X$, in which we denote $a(g,x)$ by $g(x)$, such that if $g_1, g_2 \in G$ and $x \in X$ then $g_1(g_2(x)) = (g_1g_2)(x)$ and $1_G(x) = x$.* — **[2E,B]**

(b) Given an action of G on X and an element $x \in X$, define the *stabiliser* $\mathrm{Stab}_G(x)$ and show that it is a subgroup of G. [3]

A. $\mathrm{Stab}_g(x) = \{g \in G \mid gx = x\}$. *It is a subgroup because it is not empty since $1x = x$, and if $g, h \in \mathrm{Stab}_G(x)$ then $x = hx$ so $h^{-1}x = h^{-1}hx = 1x = x$ and $ghx = gx = x$.* — **[1+2E,B]**

(c) Give an example of an action of a group G on a set X and an $x \in X$ such that $\mathrm{Stab}_G(x)$ is not a normal subgroup of G. [1]

A. *For instance, the stabiliser of 3 in S_3 is of order 2 generated by (12), but $(123)(12)(132) = (23)$ does not stabilise 3.* — **[1,S]**

(d) Show that if y is in the orbit of x then $\mathrm{Stab}_G(y)$ is conjugate to $\mathrm{Stab}_G(x)$: that is, $g\,\mathrm{Stab}_G(y)g^{-1} = \mathrm{Stab}_G(x)$ for some $g \in G$. [2]

A. *If $y \in \mathrm{orb}(x)$ then $y = gx$ for some $g \in G$ so if $h \in \mathrm{Stab}_G(y)$ then $g^{-1}hgx = g^{-1}hy = g^{-1}y = x$ so $g^{-1}\,\mathrm{Stab}_G(y)g \subset \mathrm{Stab}_G(x)$, and the other inclusion is similar.* — **[2,S]**

2. In this question, R is a commutative ring.

(a) Define what it means for a subset M of R to be a *maximal ideal*. [2]

A. *M is an maximal ideal if it is an ideal (so nonempty and closed under taking linear combinations over R) and if J is an ideal that contains M then $J = M$ or $J = R$.* — **[2E,B]**

(b) Suppose I is an ideal in R. Show that I is a maximal ideal if and only if $I + aR = R$ for every $a \notin I$. [3]

A. *If I is maximal then $I + aR = R$ because $I + aR \supset I$ (and is an ideal) and $I + aR \ni a$ so $I + aR \neq I$. Conversely, if J is an ideal strictly containing I we take $a \in J \setminus I$ and then $R = I + aR \subseteq J \subseteq R$ so $J = R$.* — **[1+2E,S]**

(c) Now let $R = K[x, y]$, where K is a field. Let a, $b \in K$. Show that the ideal I given by $I = \{f \in K[x, y] \mid f(a, b) = 0\}$ is a maximal ideal of R. [3]

A. *Put $P = (a, b)$. Then $I = \mathrm{Ker}\,\mathrm{ev}_P$ so $R/I \cong \mathrm{Im}(ev_P)$, but ev_P maps R to K and is surjective because $\mathrm{ev}_P(1) = 1$, so the quotient is a field so I is maximal.* — **[3,U]**

3. In this question, R is a commutative ring.

(a) For I and J ideals of R, define $I+J$ and IJ. [3]

A. *$I+J=\{a+b\in R \mid a\in I, b\in J\}$ and*

$$IJ := \left\{ \sum_{i=1}^{k} a_i b_i \in R \mid k\in\mathbb{N},\, a_i\in I,\, b_i\in J \text{ for all } 1\le i\le k \right\}.$$

— **[3E,B]**

(b) State the Chinese Remainder Theorem for commutative rings. [1]

A. *Let I, J be ideals in a commutative ring R satisfying $I+J=R$. Then there is a ring isomorphism $\frac{R}{I\cap J}\cong\frac{R}{I}\times\frac{R}{J}$.* — **[1E,B]**

(c) Define the *characteristic* $\operatorname{char} R$ of a commutative ring R. If S is also a commutative ring and $\operatorname{char} R=m$ and $\operatorname{char} S=n$, what can you say about $\operatorname{char}(R\times S)$? [2]

A. *$\operatorname{char} R$ is the order of 1 in the abelian group $(R,+)$. If $r1_{R\times S}=0$ then $r1_R=0_R$ and $r1_S=0_S$ (and conversely), so $m|r$ and $n|r$. Therefore $\operatorname{char}(R\times S)=\operatorname{lcm}(m,n)$ (which is 0 if $m=0$ or $n=0$).* — **[2,U]**

(d) If I and J are ideals in R, show that $\operatorname{char}\left(\frac{R}{I}\times\frac{R}{J}\right)=\operatorname{char}\left(\frac{R}{I\cap J}\right)$. [2]

A. *We cannot use CRT but $r=0$ in R/I if and only if $r1\in I$, so $r=0$ in $\frac{R}{I}\times\frac{R}{J}$ iff it is 0 in R/I and 0 in R/J iff $r1\in I\cap J$. The characteristic is the smallest such r and that is also the definition of $\operatorname{char}(\frac{R}{I\cap J})$.* — **[2,U]**

Section B

4. (a) Define what it means for a commutative ring R to be a *unique factorisation domain* (abbreviated *UFD*). [2]

A. *R is a UFD if it is a domain in which every nonzero nonunit element can be written as the product of finitely many irreducibles in R; and given two such decompositions, say $r_1 \cdots r_s = r'_1 \cdots r'_t$ we have that $s = t$ and, after renumbering if necessary, we have $r_i R = r'_i R$ for $1 \le i \le s$.* — **[2E,B]**

(b) Explain briefly why $K[x_1, \ldots, x_n]$ is a UFD for any field K. [2]

A. *We know that if R is a UFD then $R[t]$ is also a UFD. Also a field is a UFD, and $K[x_1, \ldots, x_n] \cong K[x_1, \ldots, x_{n-1}][x_n]$ so the result follows by induction on n.* — **[2E,S]**

(c) State and prove Eisenstein's criterion for irreducibility of polynomials with integer coefficients. [6]

A. *Suppose that $f = \sum_{i=0}^{d} a_i x^i \in \mathbb{Z}[x]$ is of degree d and for some prime $p \in \mathbb{Z}$ we have $p | a_i$ for $0 \le i < d$ but p does not divide a_d and p^2 does not divide a_0. Then f is irreducible in $\mathbb{Z}[x]$ (and therefore irreducible in $\mathbb{Q}[x]$). For the prrof: suppose that f is reducible in $\mathbb{Z}[x]$, so $f = gh$. Then, $\mathrm{red}_p f = (\mathrm{red}_p g)(\mathrm{red}_p h)$, but $\mathrm{red}_p f = \bar{a_d} x^d$ by the hypotheses. Since $\mathbb{F}_p[x]$ is a UFD it follows that $\mathrm{red}_p g = bx^{\deg g}$ and $\mathrm{red}_p h = cx^{\deg h}$ for some $b, c \in \mathbb{F}_p$. In particular the constant terms of $\mathrm{red}_p g$ and $\mathrm{red}_p h$ are both zero, so the constant terms of g and h are both divisible by p. But then the constant term a_0 of f is divisible by p^2.* — **[4+2E,B]**

(d) Show that each of the following polynomials with integer coefficients is irreducible.

(i) $x^4 + 14x^3 - 49x^2 + 84x - 14$. [2]

A. *This is Eisenstein with $p = 7$.* — **[2,U]**

(ii) $x^4 + 4x^2 - 7$. [3]

A. *This has no rational roots because $t^2 + 4t - 7$ has none, so if it factorises it is as $(x^2 + ax + b)(x^2 + cx + d)$, giving $a + c = 0$ from the x^3 term and $ad + bc = 0$ from the x term, as well as $bd = -7$. So $a(d - b) = 0$ so $a = 0 = c$ or $d = b$, but $d = b$ is impossible because $bd = -7$. That leaves the possibilities $(x^2 + 7)(x^2 - 1)$ and $(x^2 - 7)(x^2 + 1)$, and neither works.* — **[3,U]**

(iii) $x^4 + 7x^3 - 49x^2 + 73x - 21$. [3]

A. *Put $x = y + 1$: then we get $y^4 + 11y^3 - 22y^2 + 11$ which is Eisenstein for $p = 11$.* – **[3,U]**

5. In this question, R is an integral domain.

(a) Define what is meant by a *valuation* on R, and what is meant by a *Euclidean valuation*. [4]

A. *A valuation is a function $\nu\colon R \to \mathbb{N} \cup \{-\infty\}$ such that $\nu(a) = -\infty$ if and only if $a = 0$, and for any $a, b \in R$ we have $\nu(ab) \geq \nu(a)$. It is a Euclidean valuation if, furthermore, for any nonzero $a, b \in R$ there exist $q \in R$ and $r \in R$ with $\nu(r) < \nu(b)$, such that $a = qb + r$.* — **[4E,B]**

(b) Define what it means for R to be a *principal ideal domain* (abbreviated *PID*), and what it means for R to be a *Euclidean domain*. [2]

A. *R is a PID if every ideal is of the form aR for some $a \in R$. It is a Euclidean domain if it has a Euclidean valuation.* — **[2E,B]**

(c) Show that if R is a Euclidean domain then R is a PID. [4]

A. *Denote the Euclidean valuation on R by ν and suppose I is a nonzero ideal in R. Consider the image $\nu(I \smallsetminus \{0\})$, i.e. $\{\nu(a) \in \mathbb{N} \mid a \in I,\, a \neq 0\}$. This is a nonempty subset of $\mathbb{N}$, so it has a least element σ. Choose $b \in I$ such that $\nu(b) = \sigma$. Then if $a \in I$ there exist $q, r \in R$ such that $a = qb + r$, and $r = 0$ or $\nu(r) < \nu(b) = \sigma$. But if $r \neq 0$ then $r = a - qb \in I$, so $\nu(r) > \sigma$. This is a contradiction, so we must have $r = 0$, but then $a = qb \in bR$. Since a was arbitrary, that means $I \subseteq bR$; but $b \in I$ so we also have $bR \subseteq I$. Hence $I = bR$ and so I is a principal ideal.* — **[4,B]**

(d) Suppose that R is a PID and S is a subring of R containing 1_R. Is S necessarily a PID? Give a proof or counterexample. [2]

A. *A field is a PID so we may take $R = \mathbb{C}$ and $S = \mathbb{Z}[\sqrt{-5}]$: we know that S is not a PID.* — **[2,S]**

(e) Suppose that R is a PID and I is a prime ideal of R, with $I \neq R$. Is the quotient ring R/I necessarily a PID? Give a proof or counterexample. [3]

A. *Yes. R/I is a domain because I is prime. If J is an ideal in R/I we look at $\tilde{J}$, the preimage of J in R. It is an ideal, and since R is a PID we may assume $\tilde{J} = aR$ and then J is generated by $a + I$.* **[3,U]**

(f) By considering the ring $\mathbb{R}[x, y]$, or otherwise, give an example of a valuation that is not a Euclidean valuation. [3]

A. *The total degree function is a valuation, but it cannot be a Euclidean valuation because $\mathbb{R}[x, y]$ is not a PID: the ideal $\langle x, y \rangle$ is not principal, for instance.* — **[3,U]**

6. In this question, G is a group.

(a) Suppose that $S \subseteq G$ is a subset. Say, in terms of elements, what is meant by the *subgroup* $\langle S \rangle$ *generated by* S. [2]

A. *It is the group consisting of all products of elements of S and their inverses, i.e.* $\langle S \rangle = \{s_1 \dots s_k \mid k \in \mathbb{N},\ s_i \in S \text{ or } s_i^{-1} \in S\}$. — **[2E,B]**

(b) Show that $\langle S \rangle$ is equal to the intersection of all subgroups of G that contain S. [3]

A. *If a subgroup H of G contains S then it contains $\langle S \rangle$ because H is closed under the group operations. Hence $\langle S \rangle$ is contained in this intersection. On the other hand an element that is in all subgroups of G that contain S is in $\langle S \rangle$ as that is one of those subgroups. So $\langle S \rangle$ contains the intersection.* — **[3E,S]**

(c) Is it true that if S_1 and S_2 are subsets of G then $\langle S_1 \cap S_2 \rangle = \langle S_1 \rangle \cap \langle S_2 \rangle$? Give a proof or a counterexample. [2]

A. *No. If η is a generator of a cyclic group C of order > 2 then $\langle \{\eta\} \rangle = \langle \{\eta^{-1}\} \rangle = C$ but $\{\eta\} \cap \{\eta^{-1}\} = \varnothing$ and $\langle \varnothing \rangle = 1$.* — **[2,U]**

(d) Suppose that $S \subseteq G$ and $gSg^{-1} \subseteq S$ for all $g \in G$. Does it follow that $\langle S \rangle$ is a normal subgroup of G? Give a proof or a counterexample. [3]

A. *Yes. One way to see this is to say that $gs_1 \dots s_k g^{-1} = (gs_1g^{-1}) \dots (gs_kg^{-1})$ and if $s_i \in S$ then $gs_ig^{-1} \in S$, while if $s_i^{-1} \in S$ then $(gs_ig^{-1})^{-1} = gs_i^{-1}g^{-1} \in S$.* — **[2+1E,U]**

(e) If $a, b \in G$ then the *commutator* of a and b, denoted $[a, b]$, is the element

$$[a, b] = aba^{-1}b^{-1} \in G.$$

Let $C \subseteq G$ be the set of all commutators, i.e. $C = \{[a, b] \mid a, b \in G\}$. Show that the *derived subgroup* $G' = \langle C \rangle$ is a normal subgroup of G and that G/G' is abelian. [4]

A. *We use (d), noting that $g[a, b]g^{-1} = [gag^{-1}, gbg^{-1}]$. Hence G' is a normal subgroup. Moreover, in any group, $[a, b] = 1$ if and only if $ab = ba$ and applying that to G/G' we get $[aG', bG'] = [a, b]G' = 1_{G/G'}$ so aG' and bG' commute, so G/G' is abelian.* — **[4,U]**

(f) What is the derived subgroup of the symmetric group S_n, for $n \geq 3$? Justify your answer briefly. *[Hint: compute some commutators, and remember that every even permutation is a product of cycles of length 3.]* [4]

A. *Notice first that $[\sigma, \tau]$ is an even permutation for any $\sigma, \tau \in S_n$, because, writing ε for signature, $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)^{-1} = \varepsilon(\sigma)$ so $\varepsilon([\sigma, \tau]) = (\varepsilon(\sigma)\varepsilon(\tau))^2 = 1$. So $G' < A_n$. But G' contains all 3-cycles since $[(12), (13)] = (123)$ and the 3-cycles generate A_n.* — **[4,U]**